



TITLE:

記憶付き可逆論理素子の能力の階層構造について (アルゴリズムと計算理論の新展開)

AUTHOR(S):

向井, 優太; 森田, 憲一

CITATION:

向井, 優太 ...[et al]. 記憶付き可逆論理素子の能力の階層構造について (アルゴリズムと計算理論の新展開). 数理解析研究所講究録 2012, 1799: 167-170

ISSUE DATE:

2012-06

URL:

<http://hdl.handle.net/2433/172983>

RIGHT:

記憶付き可逆論理素子の能力の階層構造について

向井 優太*, 森田 憲一*
* 広島大学大学院工学研究科

概要

可逆コンピュータを構成するための基本素子として記憶付き可逆論理素子が研究されている。特に、素子の能力の重要な指標である万能性について多くの研究が行われている。任意の記憶付き可逆論理素子をシミュレートできることを万能という。これまで、 $k > 2$ について全ての非縮退 2 状態 k 記号可逆論理素子が万能であること、そして一部の非縮退 3 状態 2 記号可逆論理素子が万能であることが示されていた。したがって、万能な 2 状態 2 記号可逆論理素子が存在するか否かが大きな課題となっている。本稿では、2 状態 2 記号可逆論理素子 4 つの内、3 つの素子が非万能であることを示した。またこの結果は、記憶付き可逆論理素子の能力に真の階層構造が存在することも意味している。

1 はじめに

可逆論理素子は、その動作関数が単射であり、したがって現在の状態と出力から、1 時刻前の状態と入力が一意に決定できる性質を持った素子である (ただし可逆論理ゲートの場合は状態の概念がない)。可逆論理素子には、記憶機能を持つものと持たないものの 2 種類が考えられる。記憶機能を持たないもの、すなわち可逆論理ゲートの研究は Toffoli [6, 7], および Fredkin, Toffoli [2] により物理的可逆性との関連で研究され、Toffoli ゲート [6] と Fredkin ゲート [2] が共に論理万能であることが示された。他方, Morita [3] により、1 ビットの記憶を持つ可逆論理素子の一種であるロータリー素子が提案され、この素子を用いて可逆チューリングマシンを構成できることが示された。また、この構成では信号を同期させる必要がなく、可逆論理ゲートによるものより単純に実現できる。

ロータリー素子は、2 つの状態と 4 つの入出力を持つ 2 状態 4 記号記憶付き可逆論理素子の一種である。任意の記憶付き可逆論理素子について、その素子をシミュレートする回路を構成できるような素子を万能であると呼ぶ。これまで、 $k > 2$ について全ての非縮退 2 状態 k 記号素子が万能であること [4], そして一部の非縮退 3 状態 2 記号素子が万能であることが示されている [8]。したがって、2 状態 2 記号素子に万能なものが存在するか否かが大きな課題である。本稿では、非縮退 2 状態 2 記号素子 4 つのうち、2-2-2, 2-2-3 および 2-2-4 の 3 つの素子が非万能であることを示す。

2 準備

定義 1 有限状態機械 M を次のように定義する。
 $M = (Q, \Sigma, \Gamma, \delta)$, ただし Q は状態の有限集合, Σ 及び Γ はそれぞれ入力記号, 出力記号の有限集合, $\delta: Q \times \Sigma \rightarrow Q \times \Gamma$ は写像であり遷移関数と呼ぶ。また、 δ が単射であるとき M を可逆有限状態機械と呼ぶ。

ここで δ をもとに、 $\delta_1: Q \times \Sigma \rightarrow Q$, $\delta_2: Q \times \Sigma \rightarrow \Gamma$ を次のように定める。

$$\forall p, q \in Q, \forall s \in \Sigma, \forall t \in \Gamma:$$

$$\delta_1(p, s) = q \wedge \delta_2(p, s) = t \text{ iff } \delta(p, s) = (q, t)$$

$\delta_1, \delta_2, \delta$ を次のように拡張したものを $\delta_1^*: Q \times \Sigma^* \rightarrow Q$, $\delta_2^*: Q \times \Sigma^* \rightarrow \Gamma^*$, $\delta^*: Q \times \Sigma^* \rightarrow Q \times \Gamma^*$ とする。

$$\forall q \in Q, \forall s \in \Sigma, \forall \sigma \in \Sigma^*:$$

$$\delta_1^*(q, \varepsilon) = q$$

$$\delta_1^*(q, \sigma s) = \delta_1(\delta_1^*(q, \sigma), s)$$

$$\delta_2^*(q, \varepsilon) = \varepsilon$$

$$\delta_2^*(q, \sigma s) = \delta_2^*(q, \sigma) \cdot \delta_2(\delta_1^*(q, \sigma), s)$$

$$\delta^*(q, \sigma) = (\delta_1^*(q, \sigma), \delta_2^*(q, \sigma))$$

以下では、上記のように拡張した $\delta_1^*, \delta_2^*, \delta^*$ をあらためて $\delta_1, \delta_2, \delta$ と書く。

記憶付き可逆論理素子は、可逆有限状態機械の個々の入出力記号についてそれぞれ対応する入出力線を持つような論理素子とする。可逆有限状態機械 $M = (Q, \Sigma, \Gamma, \delta)$ に対応する素子は、状態 $q \in Q$ のとき $s \in \Sigma$ に対応する入力線から信号を受けると、 $\delta(q, s) = (t, p)$ のとき、状態 p に遷移して t に対応する出力線へ信号を送り出す動作を行う。以降は、 M を単に記憶付き可逆論理素子と呼ぶ。また、本稿では $|\Sigma| = |\Gamma|$ であるような素子を対象とする。すなわち入出力線数はそれぞれ $|\Sigma|$ であり、これを記号数と呼ぶ。

n 状態 m 記号素子 $M = (Q, \Sigma, \Gamma, \delta)$ は、 $Q = \{q_1, \dots, q_n\}$, $\Sigma = \{s_1, \dots, s_m\}$, $\Gamma = \{t_1, \dots, t_m\}$ に固定したとき、 δ を $(\delta(q_1, s_1), \delta(q_1, s_2), \dots, \delta(q_n, s_m))$ という列で表現できるため、これを辞書順に並べたときの番号 k を用いてその素子を n 状態 m 記号 k 番素子と呼び、 n - m - k と表記する。 n 状態 m 記号素子は、0 番から $(|Q| \times |\Sigma|)! - 1$ 番まで存在する。

記憶付き可逆論理素子は状態数と記号数が比較的小さいものでも多数存在する。しかし、その中には

記号名や状態名を付け替えるだけで同じ素子になるようなものが存在し、それらは等価であるとみなせる。そのため、等価な素子の集合からそれぞれ最も番号の小さなものを選んで代表素子と呼び、以降は代表素子のみを扱う。さらに、より少ない状態数あるいは記号数の素子と同じ動作を行う素子が存在する。そのような素子を縮退していると呼ぶ。縮退素子は、その形式上の状態数、記号数を持つ素子として扱う必要がなく、考察の対象から外してよい。

2 状態 2 記号可逆論理素子のうち非縮退で代表のものは、2-2-2, 2-2-3, 2-2-4 および 2-2-17 の 4 つである [5]。これらの素子を表す M_{2-2-2} , M_{2-2-3} , M_{2-2-4} および M_{2-2-17} を次のように定義する。

$$M_{2-2-2} = (\{q_0, q_1\}, \{a, b\}, \{x, y\}, \delta^{2-2-2}),$$

$$\delta^{2-2-2} = \left\{ \begin{array}{l} ((q_0, a), (q_0, x)), ((q_0, b), (q_1, x)), \\ ((q_1, a), (q_0, y)), ((q_1, b), (q_1, y)) \end{array} \right\}$$

$$M_{2-2-3} = (\{q_0, q_1\}, \{a, b\}, \{x, y\}, \delta^{2-2-3}),$$

$$\delta^{2-2-3} = \left\{ \begin{array}{l} ((q_0, a), (q_0, x)), ((q_0, b), (q_1, x)), \\ ((q_1, a), (q_1, y)), ((q_1, b), (q_0, y)) \end{array} \right\}$$

$$M_{2-2-4} = (\{q_0, q_1\}, \{a, b\}, \{x, y\}, \delta^{2-2-4}),$$

$$\delta^{2-2-4} = \left\{ \begin{array}{l} ((q_0, a), (q_0, x)), ((q_0, b), (q_1, y)), \\ ((q_1, a), (q_0, y)), ((q_1, b), (q_1, a)) \end{array} \right\}$$

$$M_{2-2-17} = (\{q_0, q_1\}, \{a, b\}, \{x, y\}, \delta^{2-2-17}),$$

$$\delta^{2-2-17} = \left\{ \begin{array}{l} ((q_0, a), (q_1, x)), ((q_0, b), (q_1, y)), \\ ((q_1, a), (q_0, y)), ((q_1, b), (q_0, x)) \end{array} \right\}$$

また、これらの素子は図 1 のように表現できる。例えば 2-2-2 の場合、 $\delta^{2-2-2}(q_0, a) = (q_0, x)$ は、図中の q_0 と書かれた側の a の矢印と x の矢印を繋ぐ点線に対応する。このように、四角の中に書かれた矢印を繋ぐ線はその状態毎の入力と出力の対応を、すなわち信号の進み方を示している。信号が点線を通る場合は素子の状態は変化せず、実線を通る場合はもう一方の状態に遷移する。以上のようにすることで、この表記によって素子を一意に表すことができる。

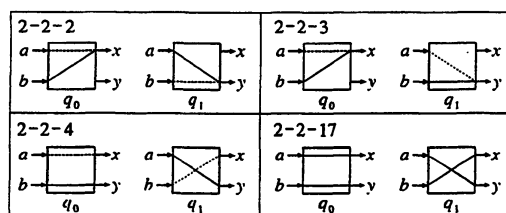


図 1: 2 状態 2 記号可逆論理素子の非縮退代表素子 [5].

本稿では、記憶付き可逆論理素子の回路を次の 2 つの制約を満たすように構成したものとする。まず、回路中の任意の接続線は、ある素子のある入力とある素子のある出力を一对一で接続する。これにより、回路中の信号の数が増減することなく、可逆性に加えて保存性も満たす。回路中の素子の接続されていない入力と出力は、それぞれその回路の入力と出

力である。次に、回路への入力直前の入力に対する出力が得られた後に与えるものとする。すなわち回路中の信号の数を高々 1 と制限する。したがって、信号の同期を考慮する必要がなく、信号の速度も任意でよい。これらの制約のもとでも、任意の可逆チューリングマシン [1] をロータリー素子と呼ばれる素子 2-4-289 のみを用いた回路でシミュレートできることがわかっている [3]。

上記の制約を満たすように記憶付き可逆論理素子の回路を次のように定義する。回路 C は、 n 個の記憶付き可逆論理素子 $M_{\text{list}} = (M_i = (Q_i, \Sigma_i, \Gamma_i, \delta^i))_{1 \leq i \leq n}$ 、それぞれ m 個の回路の入出力ポート $I = \{i_1, \dots, i_m\}$, $O = \{o_1, \dots, o_m\}$ 、及び接続 E ,

$$E: I \cup \left(\bigcup_{i=1}^n \{i\} \times \Gamma_i \right) \Rightarrow O \cup \left(\bigcup_{i=1}^n \{i\} \times \Sigma_i \right),$$

の 4 組 $C = (M_{\text{list}}, I, O, E)$ で表す。ただし、 (i, s) は M_i の入力 $s \in \Sigma_i$ に、 (i, t) は M_i の出力 $t \in \Gamma_i$ にそれぞれ対応し、 $E(a) = b$ は a と b が接続されていることを意味する。可逆論理回路においては、 E を全単射に制限する。したがって、 $E(a) = b$ のとき $E^{-1}(b) = a$ である。

また、ある回路の入出力とある素子の入出力を対応付け、任意の入力列に対してそれら 2 つの出力列が等しいとき、その回路、もしくは回路を構成する素子の集合はその素子をシミュレートするという。ある素子、あるいは素子の集合について、任意に与えられた記憶付き可逆論理素子に対してその素子をシミュレートする回路を構成できるとき、その素子、あるいは素子の集合を万能であるという。

3 非万能な記憶付き可逆論理素子

2-2-2, 2-2-3 および 2-2-4 が非万能であることを示す。

定理 2 2-2-2 は、2-2-3, 2-2-4 および 2-2-17 をシミュレートできない。

証明

任意に与えられた、 n 個の 2-2-2 を用いた回路 $C = ((M_1, \dots, M_n), \{i_1, i_2\}, \{o_1, o_2\}, E)$ 、ただし $M_i = M_{2-2-2}$ 、について、その頂点集合

$$V = \{i_1, i_2, o_1, o_2\} \cup \left(\bigcup_{i=1}^n \{i\} \times \{a, b\} \right) \cup \left(\bigcup_{i=1}^n \{i\} \times \{x, y\} \right)$$

を次のように V_1 と V_2 に分割できる。

$$\left\{ \begin{array}{l} i_1 \in V_1. \\ \forall v \in \{i_1, i_2\} \cup \left(\bigcup_{i=1}^n \{i\} \times \{x, y\} \right) \\ \quad [v \in V_1 \Leftrightarrow E(v) \in V_1]. \\ (i, a) \in V_1 \Leftrightarrow (i, x) \in V_1. \\ (i, b) \in V_1 \Leftrightarrow (i, y) \in V_1. \\ V_2 = V - V_1. \end{array} \right.$$

$i_2 \in V_2$ になること, そして V_1 と V_2 への所属について, o_1 と o_2 で異なることは容易に確認できる. o_1 と o_2 について, V_1 に属するものを o'_1 , そして V_2 に属するものを o'_2 と置く. 次に, $i \in \{1, \dots, n\}$ を, M_i の入出力の頂点 (i, a) , (i, b) , (i, x) , (i, y) が全て V_1 に属するもの, 全て V_2 に属するもの, そして V_1 と V_2 への所属が分かれるものの 3 種類に分割する. それぞれ,

$$\begin{aligned} A_1 &= \{i \in \{1, \dots, n\} \mid (i, a) \in V_1 \wedge (i, x) \in V_1\}, \\ A_2 &= \{i \in \{1, \dots, n\} \mid (i, a) \in V_2 \wedge (i, x) \in V_2\}, \\ A_3 &= \{i \in \{1, \dots, n\} \mid i \notin A_1 \cup A_2\} \end{aligned}$$

とする. 以上を図示すると図 2 のようになる.

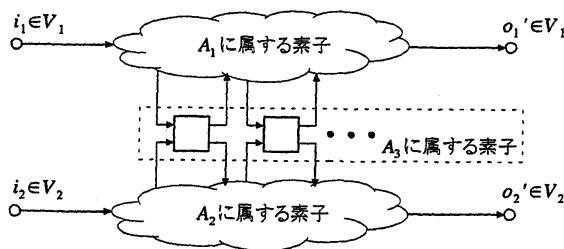


図 2: 2-2-2 回路の分割.

以上の分割方法と 2-2-2 の遷移関数より次のことがいえる.

- A_3 に属する素子でのみ信号は V_1 から V_2 へ, もしくは V_2 から V_1 へ移動できる.
- A_3 に属する素子について, ある状態の時は V_1 から V_1 への移動と V_2 から V_1 への移動のみが可能で, もう一方の状態の時は V_2 から V_2 への移動と V_1 から V_2 への移動のみが可能である.
- A_3 に属する素子について, V_1 , V_2 間を信号が移動したときかつそのときに限り, その素子の状態はもう一方へ遷移する.
- 信号が i_1 から o'_2 へ移動するとき, その間に信号が V_1 から V_2 へ移動する回数は V_2 から V_1 へ移動する回数より丁度 1 回多い.

以上より, i_1 から o'_2 という入出力の度に, A_3 に属する素子の内 V_1 から V_2 へ移動できる状態の素子が丁度 1 つ減り, V_2 から V_1 へ移動できるような素子が丁度 1 つ増えることがいえる. i_2 から o'_1 という入出力についても, 同様に上記と反対のことがいえる. したがって, A_3 は有限であるため, 回路 C の動作は, i_1 から o'_2 という入出力の回数と i_2 から o'_1 という入出力の回数の差が有限でなくてはならない.

2-2-3, 2-2-4 および 2-2-17 はそれぞれ次のような動作が可能である.

$$\delta_2^{2-3}(q_0, bbbbbb \dots) = xyxyxy \dots$$

$$\delta_2^{2-4}(q_0, bababa \dots) = yyyyyy \dots$$

$$\delta_2^{2-17}(q_0, bbbbbb \dots) = xyxyxy \dots$$

このような動作は, これらの素子の入出力と C の入出力 i_1, i_2, o'_1, o'_2 をどのように対応付けても, i_1 から o'_2 という入出力の回数と i_2 から o'_1 という入出力の回数の差を任意に大きくできる. したがって, 2-2-2 では 2-2-3, 2-2-4 および 2-2-17 をシミュレートできない. \square

定理 3 2-2-3 は, 2-2-4 および 2-2-17 をシミュレートできない.

証明

n 個の 2-2-3 による回路 $C = ((M_1, \dots, M_n), \{i_a, i_b\}, \{o_x, o_y\}, E)$, ただし $M_i = M_{2-2-3}$, が 2-2-4 をシミュレートすると仮定する. ここで, 2-2-4 すなわち M_{2-2-4} と C の入出力は, a と i_a, b と i_b, x と o_x, o と o_y がそれぞれ対応するものとする. また以降の議論は 2-2-4 を 2-2-17 に置き換えても成立する. M_{2-2-4} は次のような動作ができる.

$$\delta_2^{2-4}(q_0, bababa \dots) = yyyyyy \dots$$

回路 C の状態は回路中の n 個の 2-2-3 の状態の組で表すことができる. M_{2-2-4} の q_0 に対応する回路の状態を 1 つ選び, その回路の状態を q_C と置く. このときある k が存在し, 状態 q_C の回路に対して, $i_b i_a$ を k 回繰り返した入力列を与えると回路の状態が q_C に戻る. そのような k が存在しないことは回路の可逆性に反する. またこの時の出力列は, 回路が 2-2-4 をシミュレートする仮定より i_y を $2k$ 回繰り返したものである. この $2k$ 回の入出力の動作について, 回路の頂点集合 $V = V_1 \cup V_2$, ただし

$$V_1 = \{i_a, i_b\} \cup (\bigcup_{i=1}^n \{i\} \times \{x, y\}),$$

$$V_2 = \{o_x, o_y\} \cup (\bigcup_{i=1}^n \{i\} \times \{a, b\}),$$

のうち, 信号が一度も通っていない頂点 $V' \subset V$ に注目する. 次が成立するのは明らかである.

$$\forall v_1 \in V_1 [v_1 \in V' \Leftrightarrow E^{-1}(v_1)].$$

これより, $|V' \cap V_1| = |V' \cap V_2|$ であることがいえる. 明らかに $i_a, i_b, o_y \notin V'$, $o_x \in V'$ であるため, $\{i_a, i_b, o_x, o_y\}$ の頂点の中では $|V' \cap V_2|$ に属するものが $|V' \cap V_1|$ に属するものより 1 つ多くなっている. したがって, ある M_i について,

$$|\{(i, x), (i, y)\} \cap V'| > |\{(i, a), (i, b)\} \cap V'|$$

を満たさなければならない。すなわち、 V' への所属について、 V_1 側が V_2 側より多くなければならない。

$$|\{(i, x), (i, y)\} \cap V'| = 2 \wedge |\{(i, a), (i, b)\} \cap V'| < 2$$

の場合、素子に入力された信号が消滅することになるため、

$$|\{(i, x), (i, y)\} \cap V'| = 1 \wedge |\{(i, a), (i, b)\} \cap V'| = 0$$

が成立する。

M_{2-2-3} の遷移関数より、 M_i に b が入力されたときは必ず状態がもう一方に変わり、かつ状態が変わるのは b に入力された時のみである。 $|\{(i, a), (i, b)\} \cap V'| = 0$ より $(i, b) \notin V'$ となるため、 M_i は少なくとも 1 度は状態が変わっている。さらに、回路の状態が元に戻っているという仮定より、 M_i は 2 回以上 b を入力されていることがいえる。ここで、 M_{2-2-3} の入力列に b が 2 回以上含まれるとき、その出力列に x と y が必ず両方現れることは容易に確認できる。したがって、

$$(i, b) \notin V' \Rightarrow (i, x) \notin V' \wedge (i, y) \notin V'$$

である。しかしこれは、 $|\{(i, x), (i, y)\} \cap V'| = 1$ に矛盾する。

以上より、 C が 2-2-4 あるいは 2-2-17 をシミュレートすると仮定すると矛盾が導かれ、したがって 2-2-3 は 2-2-4 および 2-2-17 をシミュレートできない。□

定理 4 2-2-4 は、2-2-3 および 2-2-17 をシミュレートできない。

証明は、2-2-3 と 2-2-4 が入出力について鏡像のような関係になることを用いると定理 3 と同様の方法でできるため省略する。

2-2-3, 2-2-4 および 2-2-17 は 2-2-2 をシミュレートすることができる [8]。この結果と定理 2, 3, 4 を合わせると、全ての非縮退 2 状態 2 記号素子の階層構造は図 3 のようになる。

4 まとめ

2-2-2, 2-2-3 および 2-2-4 それぞれについてシミュレートできない素子が存在することを証明し、これらの素子が非万能であることを示した。これは、記憶付き可逆論理素子に真の階層構造が存在することも意味している。また、2-2-3, 2-2-4 が 2-2-2 をシミュレートすることはできるが、2-2-2 が 2-2-3, 2-2-4 をシミュレートすることはできないため、非万能な素子の間にも能力差が存在することがわかる。2 状態 3 記号素子および 3 状態 2 記号素子からは万能なものが見つかったため、これらより状態数や記号数が少ない素子の中で万能である可能性のあるものは 2-2-17 のみとなり、これが未解決問題として残されている。

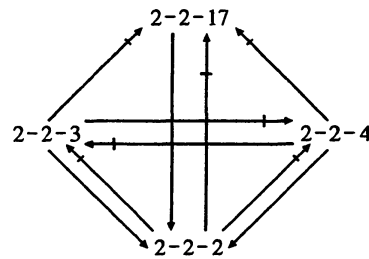


図 3: 非縮退 2 状態 2 記号可逆論理素子の階層構造。 $A \rightarrow B$ は A が B をシミュレートできることを、 $A \nrightarrow B$ は A が B をシミュレートできないことをそれぞれ示す。

参考文献

- [1] C. H. Bennett. (1973). Logical reversibility of computation. *IBM J. Res. Dev.*, 17:525–532.
- [2] E. Fredkin and T. Toffoli. (1982). Conservative logic. *Int. J. Theoret. Phys.*, 21:219–253.
- [3] K. Morita. (2001). A simple reversible logic element and cellular automata for reversible computing. In *Proc. 3rd Int. Conf. on Machines, Computations, and Universality*, LNCS 2055, pages 102–113. Springer-Verlag.
- [4] K. Morita, T. Ogiro, A. Alhazov, and T. Tanizawa. (2012). Non-degenerate 2-state reversible logic elements with three or more symbols are all universal. *J. Multiple-Valued Logic and Soft Computing*, 18:37–54.
- [5] K. Morita, T. Ogiro, K. Tanaka, and H. Kato. (2005). Classification and universality of reversible logic elements with one-bit memory. In *Proc. 4th Int. Conf. on Machines, Computations, and Universality*, LNCS 3354, pages 245–256. Springer-Verlag.
- [6] T. Toffoli. (1980). Reversible computing. In *Automata, Languages and Programming*, LNCS 85, pages 632–644. Springer-Verlag.
- [7] T. Toffoli. (1981). Bicontinuous extensions of invertible combinatorial functions. *Mathematical Systems Theory*, 14:12–23.
- [8] 向井 優太, 森田 憲一. (2011). 2 記号記憶付き可逆論理素子の万能性. In 2011 年度夏の LA シンポジウム予稿, pages S16–1–S16–15.